JCA-NET セミナー：Protonmail 入門

Protonのサイト https://proton.me

資料

(Protonmail)プライバシーポリシー

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/protonmail_privacy_policy

(Protonmail) エンド・ツー・エンド暗号化とは、どのようなもので、どのような働きをするのか？

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/protonmail-what-is-end-to-end-encryption/

(Protonmail) ミラーサイト、スパイウェア、亡命ジャーナリスト。RSFとのインタビュー

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/protonmail-world-press-freedom-day-rsf/?seq_no=5

(CLĐC)ProtonMailの開発：ProtonMailは強力なメッセージプライバシーを提供しているが、活動家が匿名性を確保するためには特別な措置が求められる

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/protonmail-developments-protonmail-provides-strong-message-privacy-but-activists-need-to-take-extra-steps-to-ensure-anonymity_jp

JCA-NET セミナー：Protonmail　入門

Protonの自己紹介のサイトから https://proton.me/about

より良い世界は、プライバシーとデジタルの自由から始まると信じています

プロトンは2014年、CERN（欧州原子核研究機構）で出会った科学者チームが、プライバシーがデフォルトとなるより良いインターネットを構築することを決意し、スイスで誕生しました。

始まりは、ワールドワイドウェブ

1991年にCERNで誕生して以来、World Wide Webは私たちの生活に革命を起こしてきました。しかし、多くの人にとって、今日のインターネットから利益を得る唯一の方法は、プライバシーよりも利益を優先する企業に膨大な量の個人データを渡すことなのです。世界の多くの地域で、政府はこのデータを悪用して市民の自由を制限しています。

プロトンは、代替手段を提供するために生まれました。

JCA-NET セミナー：Protonmail 入門

Protonの自己紹介のサイトから(つづき)https://proton.me/about

プロトンは、利益よりも人を優先するインターネットを構築し、誰もがデジタルライフをコントロールできる世界を実現し、デジタルフリーダムを現実のものにしたいという思いから生まれました。この新しい世界では、好きな人とコミュニケーションでき、自分のデータとアイデンティティを保護し、データが売られるのを避け、サイバー犯罪から保護することを可能にするのです。

私たちは、私たちが共有するビジョンを実現するために、1万人以上の個人から50万ドル以上の寄付を受けた公開クラウドファンディングを成功させ、2014年夏にプロトンを立ち上げました。それ以来、プロトンAG(スイス)は、世界中の何百万人もの人々に利用される世界有数のプライバシー企業に成長しましたが、私たちは謙虚な始まりを決して忘れてはいません。

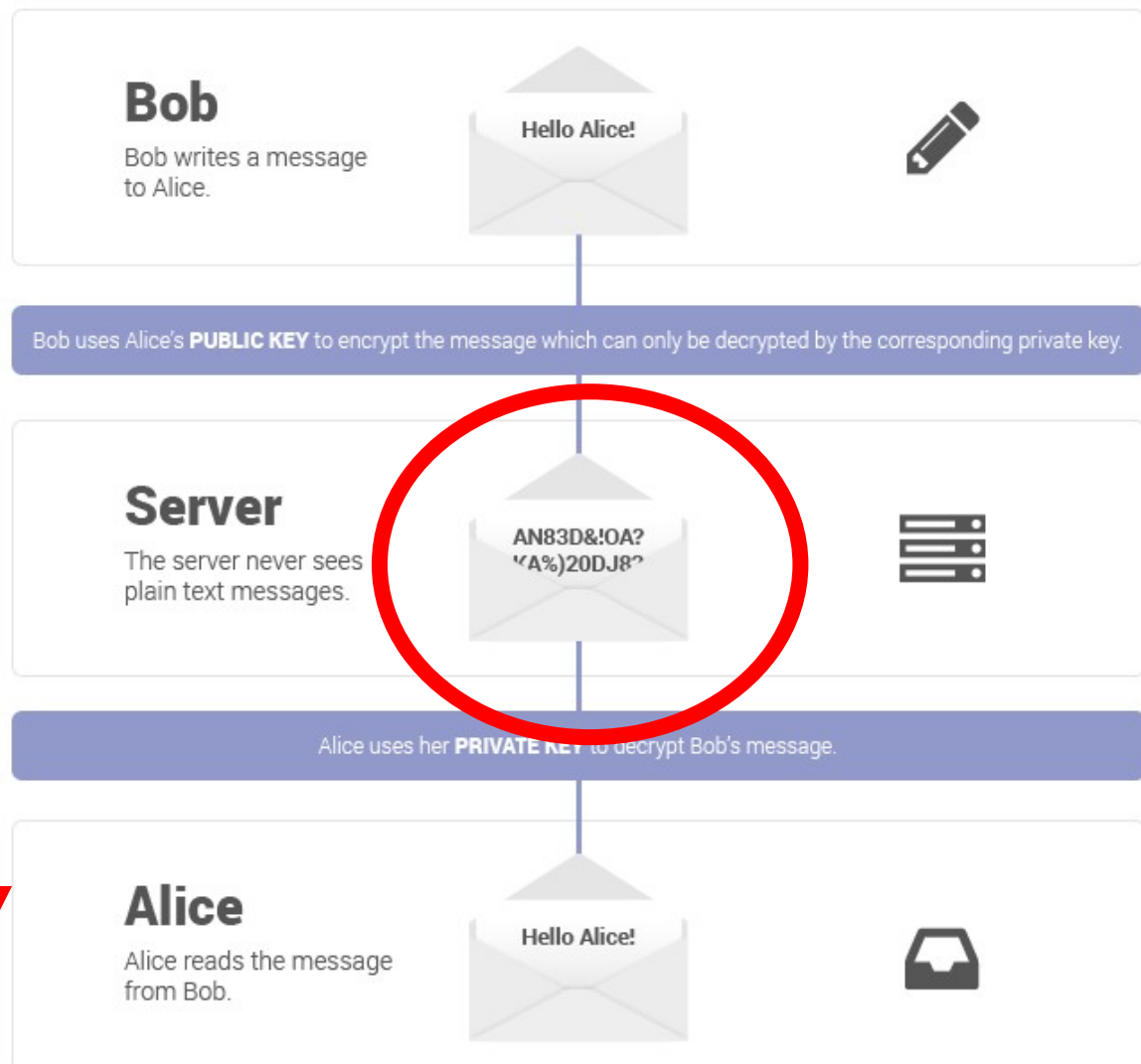
プロトンは、世界に貢献するために存在します。私たちの最初で唯一の義務は、広告主やその他の第三者ではなく、常にプロトンコミュニティに対するものです。私たちは、お客様のデータを販売することによって、お客様の信頼を損なうことはありませんし、今後もそうすることはありません。私たちは、プライバシーとオンラインの自由のために戦うことを約束し、すべての人々の利益のために役立つインターネットを守るために常に立ち上がるつもりです。

JCA-NET セミナー：Protonmail　入門

エンド・ツー・エンド暗号化(E2EE)サービスの利点

- E2EE は、ハッキングからデータを保護する。E2EE は、暗号化されていないデータにアクセスできる相手が少ないことを意味する。たとえハッカーがデータを保存しているサーバーを攻撃したとしても彼らは復号化キーを所有していないため、データを復号化することはできない。
- データのプライバシーを守ることができる。Gmail を使用している場合、Google はあなたがメールに記載した詳細な情報をすべて知ることができ、あなたがメールを削除してもメールを保存することができる。E2EE は、誰があなたのメッセージを読むかをコントロールすることができる。
- これは民主主義にとって良いことだ。誰もがプライバシーの権利を有している。E2EE は言論の自由を守り、迫害されている活動家、反体制派、ジャーナリストを脅迫から保護する。

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/protonmail-what-is-end-to-end-encryption/?seq_no=2

ボブからアリスにメールを送る。エンド・ツー・エンド暗号化メールでは、メールの送受信を管理するサーバーではメールの内容を読むことができない。

一般にメールサーバーは、扱うメールの内容を読むことが可能だ。だからメールのプライバシーは「葉書」と同等とみなされる。

JCA-NET セミナー：Protonmail　入門

ProtonMail vs Gmail

ProtonMailは、Eメールセキュリティについて、根本的に異なるアプローチをとっている暗号化されたEメールサービスである。Gmailと比較してProtonMailのセキュリティがどのようなものかを見てみよう。

2014年にProtonMailは、end-to-end暗号化によるデータ保護による世界初のEメールサービスとなった。そして、今日では世界で最も人気のある安全なEメールサービスとして世界中に数百万人のユーザがいる。

あなたのメールを読めるのはあなただけだ

ProtonMailの暗号化は、あなた以外の誰もあなたのメールボックスにあるメッセージを読むことができないことを意味している。実際、ProtonMail(の管理者)ですらあなたのメッセージを読むことはできない。他方で、Gmailはあなたの、一通一通のメールをすべて読むことができる。もし、あなたが、内密なコミュニケーションの全てに対してGoogleの無制限のアクセスを与えることに不安を感じるのであれば、ProtonMailのデータプライバシーに対するアプローチはより高い安全性を提供するだろう。

JCA-NET セミナー：Protonmail　入門

ProtonMail は万能ではない。

- スイス当局の命令でフランスの活動家の IP アドレス記録提出
- 2020 年から 2021 年にかけて、パリの Sainte Marthe 広場で再開発（高級化のためのジェントリフィケーション）に反対する建物の占拠闘争が行なわれており、厳しい弾圧を受けてきた。
- 約 20 名が逮捕され、有罪判決や数千ユーロの罰金が科せられてきた。
- 捜査の過程で、警察は「Youth For Climate」というグループが使用してきた Protonmail のアドレスと Instagram に投稿された写真に注目した。Protonmail がユーロポルを経由してスイス捜査当局の要求に応じた。

JCA-NET セミナー：Protonmail　入門

ProtonMail は万能ではない。

- プロトンはスイスの法律を遵守しなければならない。
- スイス当局からの要請に答えることがスイスの法律で義務付けられている。
- 結果として IP アドレスを提供したが、メールの本文とその他のメタデータは提出しなかった（できなかった）
- 「当社のプライバシーポリシーに記載されている項目に加えて、極端な犯罪事例 extreme criminal cases では、ProtonMail は、犯罪行為に関与している ProtonMail アカウントへのアクセスに使用されている IP アドレスを監視する義務があるかもしれない。」

JCA-NET セミナー：Protonmail　入門

ProtonMail は万能ではないが、他のメールサービスよりマシ

- Tor　経由でのアクセスで IP アドレスによる追跡を回避できる
- メール本文を盗聴されることはまずない。

Protonmail や Tutanota を使うことの「意味」

- メールのプライバシーの権利を自覚すること
- コミュニケーションの権利としての暗号化を日常の通信で実践することによって、政府の暗号規制に反対する権利を確実なものにする
- Gmail、 Yahoomail などへの依存からの脱却